REMARKS/ARGUMENTS

Prior to this amendment, claims 1-15 were pending. In this amendment, claims 1-15 are amended. No claims are canceled, and claims 16-21 are added. No new matter is added. Thus, after entry of this amendment, claims 1-21 will be pending.

Interview

Applicants would like to thank the Examiner for extending the courtesy of a telephone interview with counsel, David B. Raczkowski, on April 14, 2009, where proposed amendments provided herein were discussed.

Rejections under 35 USC § 101

Claims 14, 15 are rejected as directed toward non-statutory subject matter of only software. Applicants have amended claim 1 to recite "*hardware logic*." Accordingly, Applicants submit that claims 14-15 are directed to patentable subject matter.

Claims 1-9, 11, 12, and 14 are directed toward non-statutory subject matter. Applicants submit that these claims are directed to a practical application. For example, claim 1 recites "*generating a cryptographic key for use in a digital processing system.*" Accordingly, Applicants submit these claims are directed to patentable subject matter.

Rejections under 35 USC § 112, written description

Claims 12, 13 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. Specifically, the claim term "total" and "entire" are asserted as not appearing in the specification. To expedite prosecution, applicants have deleted these claim terms. Accordingly, Applicants respectfully request withdrawal of these claims.

Rejections under 35 USC § 103, Hoffstein, Gressel, Penner, and Fouquet

Claims 1 - 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hoffstein et al. (US Patent No. 7,031,468) in view of Gressel et al. (US Patent No. 6,748,410) and further in view of Penner (US Patent No. 7,158,569) and further in view of Fouquet ("An Extension of Fouquet's Algorithm and Its Implementation").

Claim 1

Claim 1 is allowable over the cited references, either alone or in combination, as those references fail to teach or suggest all the elements of claim 1. For example, claim 1 recites:

> *determining, with a processor, the total number of points on the elliptic curve, wherein the determining includes solving a lifted Frobenius equation to a full precision by computing a plurality of partial solutions at a plurality of successively reduced precisions, wherein the solving includes:*
>
> ...
>
> *(c) computing an error term for said lifted Frobenius equation using the first partial solution and/or a result of step (b),*
>
> ...
>
> *(e) computing, to the first reduced precision, a second partial solution of a modified lifted Frobenius equation using the error term, ...*
>
> *(1) computing, to another reduced precision, a third partial solution of said modified lifted Frobenius equation by recursively performing steps (1)-(5) to solve said modified lifted Frobenius equation from a lowest reduced precision to the another reduced precision, wherein the another reduced precision is less than the first reduced precision,*
>
> ...
>
> *(f) combining said first partial solution and said second partial solution; and*
>
> *(g) repeating steps (a)-(f) one or more additional times to solve the lifted Frobenius equation to a full precision, wherein the result from step (f) is used as the first partial solution of step (a) for the next successively higher precision.*

The Office Action states that Gressel discloses results of a first operation being used in a second operation and that Penner discloses recursive operations. Such teachings simply convey broad concepts that are very far removed from the specific operations that claim 1 recites.

For example, the use of lower precision results to obtain results at a higher precision is not mentioned anywhere. Thus, no combination of the references teach or suggest "*(f) combining said first partial solution and said second partial solution ... wherein the result from step (f) is used as the first partial solution of step (a) for the next successively higher precision*," as recited in claim 1.

Moreover, error terms of one partial solution are not used to compute "*a second partial solution of a modified lifted Frobenius equation,*" as recited in claim 1.

Additionally, claim 1 recites performing recursive calculations in a specific manner, and not simply a result of a first operation being used in a second operation. Thus, these references do not teach or suggest "*determining includes solving a lifted Frobenius equation to a full precision by computing a plurality of partial solutions at a plurality of successively reduced precisions*," as recited in claim 1.

More specifically, claim 1 recites that the second partial solution involves *recursively performing steps (1)-(5) to solve said modified lifted Frobenius equation from a lowest reduced precision to the another reduced precision*" and another recursive aspect in reciting "*repeating steps (a)-(f) one or more additional times to solve the lifted Frobenius equation to a full precision*," as recited in claim 1.

For at least these reasons, claim 1 is allowable over these references.

Claims 12-15

Applicants submit that independent claims 12 and 14, and their respective dependent claims, should be allowable for reasons mentioned with respect to claim 1.

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

CONCLUSION

In view of the foregoing, Applicants believe all claims now pending in this Application are in condition for allowance. The issuance of a formal Notice of Allowance at an early date is respectfully requested.

If the Examiner believes a telephone conference would expedite prosecution of this application, please telephone the undersigned at 415-576-0200.

Respectfully submitted,

/David B. Raczkowski/

David B. Raczkowski
Reg. No. 52,145

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, Eighth Floor
San Francisco, California 94111-3834
Tel: 415-576-0200
Fax: 415-576-0300
DBR:dbr
61912909 v1